State of Montana Information Security Advisory Council

Council Meeting Minutes
May 19, 2016
11:00 a.m.
State Capitol - Room 137

Members Present:
Ron Baldwin, CIO, Chair
Joe Chapman, DOJ
Joe Frohlich, SITSD
Stuart Fuller, DPHHS
Kreh Germaine, DNRC
Jim Gietzen, OPI
Adrian Irish, UM
Margaret Kauska, DOR
Lynne Pizzini, CISO
Maj. Gen. Matthew Quinn, DMA
Erika Billiet, City of Kalispell
Sherri Davidoff, LMG Security

Staff Present:
Jennifer Schofield
Noah Horan

Guests Present:
Brian Fox, Lisa Vasa, Michael Barbere, Sean Rivera, Eric Durkin, Craig Stewart, Daniel Nelson, Dawn Temple, Rebecca Cooper, Christie McDowell, Peder Cannon, Tim Kosena, Tom Shultz, Lance Wetzel, Darrin McLean, Christi Mock, Angie Riley

Real-time Communication:
Kyle Belcher, Zach Day, Phillip English, Mandi Hinman, Ed Sivils, Manuel Soto

Welcome and Introductions
Ron Baldwin welcomed the council to the May 19, 2016 MT-ISAC meeting. All members and guests were introduced.

Minutes
The council reviewed and approved the April 21, 2016 Minutes.

Business
MT-ISAC Scorecard Discussion
Ron Baldwin proposed that the group re-characterize the scorecard as a Progress Report. Ron and Joe Frohlich will develop a summarized sheet of goals and objectives.

Joe discussed the Progress Report, and noted that the "accomplished" language has been changed to "addressed." Joe noted that the Progress Report is to be used by the Council members to familiarize themselves with what is going on within the workgroups. Moving forward, the Council will acknowledge that objectives are being addressed. The Progress Report will be located on the website, and will be updated regularly. Joe gave a brief summary of the current items for discussion to determine whether they have been addressed.

Ron asked if the Council had comments or input.

Q: Maj. Gen. Matthew Quinn: I wonder if, as items are being addressed, we could do a change report to show what has happened from one MT-ISAC meeting to the next.

A: Ron: This is exactly what I am going to be working with Joe on.

Q: Kreh Germaine: To say that we are addressing an item in an ongoing capacity takes more than a one-time meeting with someone. Are we really being proactive?

A: Ron: The Council identifies activities to be addressed. This Council is a participatory body, so the burden is on the individual Council members to suggest activities, contribute in the workgroups, and come back to the main meeting and track these activities. The Council then determines whether the goal has been addressed, is in progress, or is planned.

National Initiative for Cybersecurity Education
Lisa Vasa discussed a funding opportunity via the National Initiative for Cybersecurity Education (NICE). They are currently soliciting applications from eligible applicants to establish Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS). These RAMPS will identify cybersecurity workforce development pathways for local workforce

needs, and will work to promote these educational opportunities by aligning the specific workforce needs of local businesses and non-profits with the learning objectives of cybersecurity education and training providers.

This funding opportunity will provide 5 to 8 grants in the total amount of $150,000 to $200,000 each for a fifteen-month project. The grant proposal deadline is July 12, 2016, and the application is to be submitted through the grants.gov program. Applicants must be a non-profit or an institution of higher education. The applicant must have a letter of commitment from one of each of the following three types of organization: a K-12 school, a higher education institution (if the applicant is not one itself), and a local employer. The specific project proposal must: identify what the partnership will be; describe how it will collaborate with centers of academic excellence in cybersecurity or with advanced technological educators; describe how the leadership and governance of the RAMPS will be established; detail what the initiatives that will meet these goals will be; demonstrate how the RAMPS will use the NICE framework; include ideas how the RAMPS will leverage the cybersecurity jobs heatmap; include employers in the community who will provide internships, apprenticeships or coop programs; and define the metrics of how the project will be measured. The full announcement is posted on the MT-ISAC website.

Q: Adrian Irish: I am curious if other potential applicants are asking for an extension of the deadline. The grant proposal is looking for a consortium of groups that do not typically work together. It would be a serious challenge to form that consortium before the deadline of July 12, 2016, much less to write the grant.

A: Lisa: I can follow up and contact NICE for more information.

Workgroup Updates

Assessment Workgroup

Joe Frohlich provided an update. On Friday, May 13, 2016, there was a meeting after NMG to discuss the Policy Assessment Tool pilot. The agencies participating are: the Department of Administration, the Department of Revenue, the Department of Transportation, the Department of Natural Resources and Conservation, and the Department of Public Health and Human Services. All agencies are welcome to join the pilot. Joe is proposing that the July MT-ISAC meeting be the end of the pilot, at which time the participating agencies will report. Once the Assessment Tool is approved, July 1, 2017 would be the deadline for reporting to the CIO.

Best Practices Workgroup

Joe Frohlich discussed some of the workgroup's recent output, including the Small Incident Handling document, which is to be used for low-level events such as malware attacks. A few small changes have been made. The document is available on the website for review.

Lynne Pizzini moved that the Council approve the Small Incident Handling document as a best practice. Stuart Fuller seconded. The voice vote was unanimous.

The Hardening of Devices document was amended to include an exception request document for use in the event that an agency cannot comply with a certain provision. Moving forward, all documents created by the Best Practices workgroup will have an exception request document included. Joe highlighted any changes made. There are two documents for review to be voted on during the June MT-ISAC meeting: The Disposal of Media Storage Device procedure, and the Large Cyber Incident Handling document.

Situational Awareness Workgroup

Joe Frohlich informed the Council that the Situational Awareness group met prior to the Best Practices group meeting in order to bring the Large Incident Handling document to Best Practices to discuss. Joe mentioned that the two workgroups worked well together in producing this document.

Tools Workgroup

Dawn Temple gave a brief overview of the Tools group's work on the Device Hardening Strategy document. Fifteen agencies are currently reporting back regarding Device Hardening, and are at varying levels of completion. Unfortunately there is little documentation on paper, so it is important to document implementation moving forward, and the sharing of such documentation, policies, or procedures is highly encouraged. Dawn also mentioned that Sean Rivera provided a number of documents for Gartner. The agencies involved produced a Key Findings document. The agencies identified two key considerations: one, the reduction of an agency's attack surface; and two, the need for better technical features in endpoint protection software. The group also compiled a list of wants vs. needs for enterprise antivirus protection. There is a need for proactive protection software, and Microsoft Endpoint is more reactive. The group recommends moving forward with a different endpoint protection software product. The funding mechanism is to be determined. The software must fit well within the enterprise security strategy.

Current Threats

Sean Rivera provided an update on Microsoft Wi-Fi Sense, an application that was introduced into the Windows 8.1 platform, and is also included in Windows 10. Wi-Fi Sense is meant to share Wi-Fi access point encryption information with friends. There was fear regarding the potential vulnerabilities this software would introduce, but nothing substantial was reported. Due to low adoption rates, Microsoft will drop the application. It will not be present in the Windows 10 Anniversary Update, which comes out this summer.

Apple updates have resolved DROWN (SSLv2) vulnerability within each of their operating systems, and also iTunes and Safari. Sean reminded the Council to always backup your device before applying patches.

Google Chrome will soon block Flash by default. HTML5 will be the primary content delivery system used in the Chrome browser by Q4 2016.

A database dump of 117 million LinkedIn account records is currently for sale on a darknet market site. The dump is valued at five bitcoins (approximately $2,200) and contains user IDs, email addresses, and SHA1 password hashes. The database in question is from 2012, and may be outdated. Sean encouraged anyone using LinkedIn to change their password and use LinkedIn's two-factor authentication option.

Adjournment

Next Meeting

June 16, 2016, 11:00 a.m.
DEQ Lee Metcalf Building, Room 111

Member Forum

Ron Baldwin asked for a brief summary of the IRS and SSA audits, which Lynne Pizzini and Margaret Kauska provided to the Council.

Margaret thanked everyone involved in preparing for the audits. The audits went well overall. Margaret appreciates the Enterprise Security Policy being in place, and although the Department of Revenue has not officially adopted it, DOR is working towards adoption.

Stuart Fuller mentioned that he found it interesting that the IRS audit seemed to focus on areas that had not previously been focused on. The auditors reacted positively to the System Security Plan templates and other assessment documents.

Lynne Pizzini appreciated being involved with the audits because she considers them helpful from a security perspective. Both our Enterprise server and storage environments received high compliance ratings: 92% for server, and 99% for storage. SITSD is transitioning to Windows 10, and those devices that have transitioned and are in compliance with the Device Hardening Strategy would have scored higher with the auditors than the Windows 7 and 8 devices that were actually inspected.

Ron solicited input for future agenda items. He mentioned that he would like to invite the CISO from Northwestern Energy to come speak to the Council about critical infrastructure.

Dawn Temple: We are still waiting for the Security Posture presentation from SITSD.
Joe Frohlich: That presentation was moved to June for scheduling reasons. There will be a panel of SITSD Bureau Chiefs who will give a quick highlight of the security areas of each bureau. Our main concern is providing ample time.
Stuart Fuller: My one concern regarding this panel presentation is that we have to run the fine line between disclosing what we do versus protecting what we do.
Lynne Pizzini: We may be closing the meeting for that presentation.

Public Comment

None.

Adjourn

The meeting adjourned at 12:30 p.m.

Adopted June 16, 2016.